ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Электронная почта и безопасность

Почти любой работающий человек в мире владеет своим электронным почтовым адресом. Электронная почта — самый простой способ для быстрой и своевременной передачи информации. В этой статье мы хотим рассказать как безопасно пользоваться электронной почтой чтоб не стать жертвой мошенников или не потерять вашу переписку.

- Рекомендуется иметь хотя-бы 3 почтовых ящика: один для рабочих контактов, другой для персональной переписки и обычный для всего остального.
- Закрывайте окна web-браузера после окончания работы, особенно если вы находитесь в библиотеках, Интернет-кафе и т.п.
- Не сохраняйте пароли в браузере и очищайте кэш браузера, историю посещённых сайтов, cookies.
- По возможности, используйте безопасные браузеры.
- Ни в коем случае не пользуйтесь обычной почтой для пересылки конфиденциальной и служебной информации.
- Не забывайте, что некоторые вопросы можно решить по телефону, а это намного безопаснее, чем использование электронной почты.

Операторская работа с электронной почтой

- При пересылке чужой корреспонденции требуется, по крайней мере редактировать текст и удалять адреса других корреспондентов. Иначе в одном письме будет сосредоточено много адресов, в результате вырастет угроза спама.
- Своевременно архивируйте корреспонденцию, в особенности если она делового содержания.
- При использовании мобильного доступа к почтовому ящику всегда знайте, остается ли на почтовом сервере копия вашего письма. В противном случае после удаления письма из телефона оно будет потеряно.
- Не забывайте, что удаление письма из папки почтового клиента вовсе не означает его удаление вообще. Письма могут годами храниться в архивных папках на удаленных серверах и в случае необходимости могут быть восстановлены специалистами.
- Не открывайте и не скачивайте сомнительный входящие письма от адресатов, которые Вам не знакомы и Вы не ожидаете от них никакой корреспонденции.
- Не переходите по ссылкам в сомнительных входящих письмах или их вложениях.
- Не предоставляйте свои персональные данные сомнительным адресатам в переписке по электронной почте, особенно если это касается данных организаций.

Борьба с вирусами, троянами и стилерами

- Не забываете, что трояны и другие вирусы могут прийти и с доверенных адресов вашей почты, к примеру, в случае если компьютер вашего приятеля заражён.
- Не уничтожайте спам сообщения, а помещайте эту корреспонденцию в черный список.
- Не отключайте спам-фильтр.
- Пользуйтесь антивирусами с включенной возможностью сканирования вложений e-mail.

Как не стать жертвой хакера

- Не делитесь данными об аккаунте с другими.
- Применяйте сложные буквенно-цифровые пароли.
- Шифруйте самые важные ваши сообщения.
- Применяйте шифрование при мобильном доступе к вашей электронной почте.
- Используйте электронную цифровую подпись для важной, деловой переписки.
- Работая на общедоступном компьютере, доступ к которому могут иметь случайные

пользователи, всегда очищайте кэш браузеров.

Это элементарные нормы безопасности при работе с электронными почтовыми ящиками!

Безопасный логин и пароль

При посещении того или иного сайта нам предлагают зарегистрироваться на нём и получить те или иные блага ресурса. Чтобы придумать логин и (или) пароль, сайты предлагают стандартные схемы с использованием заглавных букв или цифр, иногда знаков. Данная схема давно известна хакерам и недобросовестным программистам. Не надо полагать что такие хакеры сидят сутками и подбирают вручную логин и пароль к Вашему аккаунту на каком либо сайте, это делается при помощи программ-ботов, которые куда быстрее это сделают автоматически.

Какова же цель таких взломов?

На самом деле всё довольно просто. Ваши персональные данные, а именно кража средств с подключенных к аккаунту телефонов или банковских карт. Также это может быть применимо к связующим аккаунтам, пример - Ваши друзья в социальных сетях.

Что делать и как быть?

Самое главное это не использовать логины и пароли из одного слова или набора цифр по порядку. Не использовать одинаковый логин и пароль на разных аккаунтах. Использовать максимально длинные логины и пароли, состоящие из заглавных и строчных букв латинского алфавита, использовать в сочетании цифры и знаки. Но это ещё не всё. В целях повышения безопасности некоторые ресурсы используют привязку мобильного телефона, при авторизации на сайте, на мобильный телефон приходит SMS с кодом и такой код вводится в специальное поле на сайте. Также такие коды могут быть выданы заблаговременно пользователю и иметь отдельную степень безопасности. Сегодня это наверное один из наилучших способов безопасности черед SMS-код или ранее выданный. Поэтому если на сайте имеется такая опция, обязательно включите её.

Капча, что это такое?

Капча это визуальный код от спам-ботов. Бывают логические, в виде размытого цветного текста, бывают арифметические, в виде решения математического примера. Но капчи бывают и в виде мозаики нескольких изображений, из которых приходится выбирать необходимые. Последний вариант наиболее безопасный.

Не стоит пренебрегать опциями регистрации и настройками аккаунта на сайтах, это поможет сохранить не только персональные данные, но и средства.

Безопасность в сети Интернет

Безопасность в сети Интернет Сегодня огромное количество информации обрабатывают с помощью персональных или рабочих компьютеров, поэтому атаки на компьютерные системы получили большую распространенность. С каждым годом число активных пользователей Интернета растет в геометрической прогрессии, следовательно проблема безопасности при работе в сети все более актуальна. К сожалению, знания пользователей о основах компьютерной безопасности при использовании Интернет отстают от темпов развития сети и лавинообразного роста угроз безопасности. Как программное обеспечение может представлять угрозу информационной безопасности в сети Интернет? К таким угрозам мы можем отнести:

вредоносное программное обеспечение (вирусы),

интернет-мошенничество;

атаки на отказ в обслуживании;

кражи денежных средств; кражи персональных данных;

несанкционированный доступ к информационным ресурсам и систем;

распространение заведомо недостоверной информации.

Кроме того, вам уже известны основные угрозы информационной безопасности пользователя Интернета, которые идут от авторизованных пользователей и электронных методов воздействия.

От авторизованных пользователей: Умышленные повреждения или похищения данных хакерами Повреждения данных в результате неосторожных действий Электронные методы воздействия: Компьютерные вирусы Спам Фишинг Рассмотрим влияние на безопасность со стороны различного вредоносного программного обеспечения, которое распространяется по сети Интернет. Вредоносное программное обеспечение (англ. Malware, malicious software — вредоносная программа, вредоносное) — любое программное обеспечение, предназначенное для получения несанкционированного доступа к вычислительным ресурсам самого компьютера или к информационным ресурсам, которые хранятся на нем, предназначенное для несанкционированного владельцем их использования или причинение вреда (нанесение ущерба) владельцу компьютера, информации или компьютерной сети путем копирования, искажения данных, удаление или подмены информации. Термин «вредоносная программа» (malware — это сокращение от «malicious software») с трактовкой корпорации Microsoft обычно используется как общепринятый термин для обозначения любого программного обеспечения, специально созданного для того, чтобы причинять ущерб отдельному компьютеру, серверу или компьютерной сети, независимо от того, является ли оно вирусом, шпионской программой и тому подобное. Вредоносные программы по виду нанесенного ущерба можно отнести к нескольким категориям. Вредоносные программы: создают помехи в работе системы; уменьшают ресурсы компьютера; выполняют несанкционированные действия с данными; дестабилизируют работу пользователя с компьютером. Препятствиями в работе зараженного компьютера могут быть различные вредоносные действия: начиная от открытия-закрытия лотка CD-ROM и заканчивая уничтожением данных и поломкой аппаратного обеспечения; блокирование антивирусных сайтов, антивирусного программного обеспечения и административных функций операционной системы с целью усложнения их лечения; саботаж производственных процессов, управляемых компьютером (этим занимался известный червь Stuxnet). Часто зараженный файл выполняет установку другого вредоносного программного обеспечения: загрузка из сети и распаковки другой, еще более вредоносной программы, либо вредоносный код уже содержится внутри файла (dropper), часто вредоносное программное обеспечение занимает почти все ресурсы компьютера. К несанкционированным действиям с данными относят: кражу, мошенничество, вымогательство и шпионаж за пользователем. Для кражи может применяться сканирование жесткого диска, регистрация нажатий клавиш (Keylogger) и перенаправление пользователя на поддельные сайты, в точности повторяющие исходные ресурсы; похищения данных, представляющих ценность или тайну; кража аккаунтов различных служб (электронной почты, мессенджеров, игровых серверов, платежных систем). Аккаунты при этом применяются для рассылки спама, а через электронную почту можно заполучить пароли от других аккаунтов, в то время как виртуальное игровое имущество можно продать в MMOG (Massively multiplayer online game). Вредоносное программное обеспечение вызывает блокировку компьютера, шифрование файлов пользователя с целью шантажа и вымогательства денежных средств. Зачастую после оплаты компьютер либо не разблокируется, либо вскоре блокируется во второй раз. Вредоносная программа использует телефонный модуль для осуществления дорогостоящих звонков на платные номера, зарегистрированные злоумышленниками, что вызывает значительные суммы в телефонных счетах. Возможно также создание платного программного обеспечения, которое имитирует, например, антивирус, но ничего полезного при этом не делает (fraudware или scareware). Вредоносные программы также выполняют другую незаконную деятельность: получение несанкционированного доступа к ресурсам самого компьютера или третьих ресурсов, доступных через него, в т.ч. прямое управление компьютером (так называемый backdoor), осуществляют организацию на компьютере открытых vpn-туннелей и общедоступных прокси-

серверов. Зараженный компьютер (в составе ботнета) может быть использован для проведения DDoS-атак, сбор адресов электронной почты и распространение спама, в т.ч. в составе ботнета. К такой деятельности относится также накручивания электронных голосований, кликов по рекламным баннерам; генерирования монет платежной системы Bitcoin, и даже использование эффекта 25-го кадра для зомбирования человека.

Rootkit *(рутkит, от англ. Root kit, то есть «набор root'a») программа или набор программ, предназначенный для скрытия следов присутствия злоумышленника или вредоносного программного обеспечения от посторонних глаз.*

Ransomware *(от англ. Ransom — выкуп и software — программное обеспечение) — это вредоносное программное обеспечение, которое работает как вымогатель.*

Ботнет *(англ. Botnet от robot и network) — это компьютерная сеть, состоящая из некоторого количества хостов, с запущенными ботами — автономным программным обеспечением. Чаще всего бот в составе ботнета является программой, которая скрыто устанавливается на компьютере жертвы и позволяет злоумышленнику выполнять определенные действия с использованием ресурсов зараженного компьютера.*

Нежелательное программное обеспечение может записывать файлы, которые не являются истинно вредными, но в основном нежелательными: шутливое программное обеспечение, то есть которое делает какие-либо вещи, которые беспокоят пользователя. Например, программа Adware показывает рекламу, а программа Spyware посылает через сеть Интернет информацию, несанкционированную пользователем. Создается так называемое «отравления» документов, дестабилизирующее программное обеспечение, которое открывает их (например, архив размером менее мегабайта может содержать многие гигабайты данных, а при его распаковке может надолго «зависнуть» архиватор, или даже переполниться жесткий диск). Программы удаленного администрирования могут применяться как для того, чтобы дистанционно решать проблемы с компьютером, так и для вредоносных целей. Иногда вредоносное программное обеспечение для собственного «жизнеобеспечения» устанавливает дополнительные утилиты: IRC-клиенты, программные маршрутизаторы, открытые библиотеки перехвата клавиатуры. Такое программное обеспечение не является вредным, но вместе с ним устанавливается более вредоносная программа, которая определяется антивирусами. Бывает даже, что вредоносен только скрипт из одной строки, а остальная часть программы вполне легитимна.

7 базовых правил защиты от фишинга

О том, что такое фишинг известно давно. Первые фишинговые атаки были зафиксированы вскоре после появления всемирной паутины. Но несмотря на то, что специалисты по ИБ создают все более совершенные способы защиты от фишинга, новые фишинговые сайты продолжают появляться ежедневно.

Согласно данным некоторых исследований, в 2016 году ежедневно создавалось около 5000 фишинг сайтов. В 2017 эта цифра будет еще больше. Секрет жизнестойкости этого вида мошенничества в том, что он опирается не на "дыры" в программном обеспечении, а на уязвимость в человеческой сущности, у которой есть доступ к важным данным. Поэтому нелишним будет в очередной раз напомнить, что такое фишинг, каковы самые распространенные виды фишинговых атак, а также способы противодействия им.

Фишинг: основные примеры фишинговых атак

Фишинг — это вид интернет-мошенничества, построенный на принципах социальной инженерии. Главная цель фишинга — получить доступ к критически важным данным (например, паспортным), учетным записям, банковским реквизитам, закрытой служебной

информации, чтобы использовать их в дальнейшем для кражи денежных средств. Работает фишинг через перенаправление пользователей на поддельные сетевые ресурсы, являющиеся полной имитацией настоящих.

1. Классический фишинг — фишинг подмены

К этой категории можно отнести большую часть всех фишинговых атак. Злоумышленники рассылают электронные письма от имени реально существующей компании с целью завладеть учетными данными пользователей и получить контроль над их личными или служебными аккаунтами. Вы можете получить фишинговое письмо от имени платежной системы или банка, службы доставки, интернет-магазина, социальной сети, налоговой и т.д.

Фишинговые письма создают с большой скрупулезностью. Они практически ничем не отличаются от тех писем, которые пользователь регулярно получает в рассылках от настоящей компании. Единственное, что может насторожить — просьба перейти по ссылке для выполнения какого-либо действия. Переход этот, однако, ведет на сайт мошенников, являющийся “близнецом” страницы сайта банка, социальной сети или другого легального ресурса.

Побудительным мотивом для перехода по ссылке в подобных письмах может выступать как “пряник” (”Вы можете получить 70% скидку на услуги, если зарегистрируетесь в течение суток”), так и “кнут” (”Ваша учетная запись заблокирована в связи с подозрительной активностью. Чтобы подтвердить, что вы владелец аккаунта, перейдите по ссылке”)

Приведем список самых популярных уловок мошенников:

- Ваша учетная запись была или будет заблокирована /отключена.

  Тактика запугивания пользователя может быть очень эффективной. Угроза того, что аккаунт был или в ближайшее время будет заблокирован, если пользователь сейчас же не зайдет в учетную запись, заставляет тут же потерять бдительность, перейти по ссылке в письме и ввести свой логин и пароль.

- В Вашей учетной записи обнаружены подозрительные или мошеннические действия. Требуется обновление настроек безопасности.

  В таком письме пользователя просят срочно войти в учетную запись и обновить настройки безопасности. Действует тот же принцип, что и в предыдущем пункте. Пользователь паникует и забывает о бдительности.

- Вы получили важное сообщение. Перейдите в личный кабинет, чтобы ознакомиться.

  Чаще всего такие письма присылают от имени финансовых организаций. Пользователи склонны верить правдивости писем, поскольку финансовые организации действительно не пересылают конфиденциальную информацию по электронной почте.

- Фишинговые письма налоговой тематики.

  Такие письма входят в тренд, как только близится время платить налоги. Темы писем могут быть самыми разными: уведомление о задолженности, просьба выслать недостающий документ, уведомление о праве на получение возврата налога, и т.д.

2. Целенаправленная фишинговая атака

Не всегда фишинг бьет наудачу — часто атаки являются персонифицированными, целенаправленными. Цель та же — заставить пользователя перейти на фишинговый сайт и оставить свои учетные данные.

Естественно, у будущей жертвы больше доверия вызовет письмо, в котором к ней обращаются по имени, упоминают место работы, должность, занимаемую в компании, еще какие-либо индивидуальные данные. Причем информацию для направленных фишинговых атак люди чаще всего предоставляют сами. Особенно “урожайны” для преступников такие ресурсы как всем известная LinkedIn — создавая резюме в расчете на потенциальных работодателей, каждый старается указать побольше сведений о себе.

Для предупреждения подобных ситуаций организациям следует постоянно напоминать сотрудникам о нежелательности размещения личной и служебной информации в открытом доступе.

3. Фишинг против топ-менеджмента

Особый интерес для мошенников представляют учетные данные руководства.

Как правило, специалисты по безопасности любой фирмы внедряют четкую систему допусков и уровней ответственности, в зависимости от должности работника. Так, менеджер по продажам имеет доступ к базе данных продукции, а список сотрудников компании для него — запретная зона. HR-специалист, в свою очередь, полностью в курсе, какие вакансии кем заняты, какие только что освободились, кто достоин повышения, но понятия не имеет о номерах и состоянии банковских счетов родной фирмы. Руководитель же обычно сосредотачивает в своих руках доступ ко всем критически важным узлам жизни предприятия или организации.

Получив доступ к учетной записи главы компании, специалисты по фишингу идут дальше и используют ее для коммуникации с другими отделами предприятия, например, одобряют мошеннические банковские переводы в финансовые учреждения по своему выбору.

Несмотря на высокий уровень допуска, менеджеры высшего звена не всегда участвуют в программах обучения персонала основам информационной безопасности. Вот почему, когда фишинговая атака направлена против них, это может привести к особенно тяжелым последствиям для компании.

4. Фишинг рассылки от Google и Dropbox

Сравнительно недавно в фишинге появилось новое направление — охота за логинами и паролями для входа в облачные хранилища данных.

В облачном сервисе Dropbox и на Google Диске пользователи, как личные так и корпоративные, хранят множество конфиденциальной информации. Это презентации, таблицы и документы (служебные), резервные копии данных с локальных компьютеров, личные фотографии и пароли к другим сервисам.

Неудивительно, что получить доступ к учетным записям на этих ресурсах — заманчивая перспектива для злоумышленников. Для достижения этой цели используют стандартный подход. Создается фишинговый сайт, полностью имитирующий страницу входа в аккаунт на том или ином сервисе. Потенциальных жертв на него в большинстве случаев перенаправляет фишинговая ссылка в электронном письме.

5. Фишинговые письма с прикрепленными файлами

Ссылка на подозрительный сайт с целью украсть данные пользователя — не самое страшное, на что способен фишинг. Ведь в этом случае преступники получат доступ лишь к

определенной части конфиденциальной информации — логину, паролю, т.е к аккаунту в определенном сервисе. Гораздо хуже, когда фишинг-атака приводит к компрометации всего компьютера жертвы вредоносным программным обеспечением: вирусом-шифровальщиком, шпионом, трояном.

Такие вирусы могут содержаться во вложениях к письмам. Предполагая, что письмо пришло от доверенного источника, пользователи охотно скачивают такие файлы и заражают свои компьютеры, планшеты и лэптопы.

Что такое фарминг

Классический фишинг со ссылками на сомнительные ресурсы постепенно становится менее эффективным. Опытные пользователи веб-сервисов обычно уже осведомлены об опасности, которую может нести ссылка на подозрительный сайт и проявляют осмотрительность, получив странное письмо или уведомление. Заманить жертву в свои сети становится все труднее.

В качестве ответа на снижение результативности традиционных атак злоумышленниками был придуман фарминг — скрытое перенаправление на мошеннические сайты.

Суть фарминга состоит в том, что на первом этапе в компьютер жертвы тем или иным образом внедряется троянская программа. Она зачастую не распознается антивирусами, ничем себя не проявляет и ждет своего часа. Вредонос активируется лишь тогда, когда пользователь самостоятельно, без всякого внешнего воздействия, решает зайти на интересующую преступников страницу в интернете. Чаще всего это сервисы онлайн-банкинга, платежные системы и прочие ресурсы, осуществляющие денежные транзакции. Здесь-то и происходит процесс подмены: вместо проверенного, часто посещаемого сайта хозяин зараженного компьютера попадает на фишинговый, где, ничего не подозревая, указывает нужные хакерам данные. Делается это с помощью изменения кэша DNS на локальном компьютере или сетевом оборудовании. Такой вид мошенничества особенно опасен из-за трудности его обнаружения.

Защита от фишинга — основные правила

1. Обязательно проверить URL-адрес, по которому рекомендуется перейти, на наличие незначительных ошибок в написании.
2. Использовать лишь безопасные https-соединения. Отсутствие всего одной буквы “s” в адресе сайта обязано насторожить.
3. С подозрением относиться к любым письмам с вложениями и ссылками. Даже если они пришли со знакомого адреса, это не дает гарантии безопасности: он мог быть взломан.
4. Получив неожиданное подозрительное сообщение, стоит связаться с отправителем каким-либо альтернативным способом и уточнить, он ли его послал.
5. Если все же необходимо посетить ресурс, лучше ввести его адрес вручную или воспользоваться ранее сохраненными закладками (увы, от фарминга это не убережет).
6. Не использовать для доступа к онлайн-банкингу и другим финансовым сервисам открытые Wi-Fi сети: часто их создают злоумышленники. Даже если это не так, подключиться к незащищенному соединению не составляет сложности для хакеров.
7. На всех аккаунтах, где это возможно, подключить двухфакторную аутентификацию. Эта мера может спасти положение, если основной пароль стал известен взломщикам.

Выводы

Полностью уничтожить фишинг в обозримом будущем вряд ли получится: человеческая лень, доверчивость и жадность тому виной.

Ежедневно происходят тысячи фишинговых атак, которые могут принимать самые разнообразные формы:

- **Классический фишинг**. Фишинговые письма, отправленные от имени известных действительно существующих компаний, которые практически неотличимы от писем, которые пользователи обычно получают от этих компаний. Единственное отличие может заключаться в просьбе проследовать по ссылке, чтобы выполнить какое-то действие.
- **Целенаправленная фишинговая атака**. Персонализированные фишинговые письма, направленные на конкретного человека. Такие письма содержат имя, должность потенциальной жертвы, а также любые другие личные данные.
- **Фишинг против топ-менеджмента**. Фишинг-письма нацеленные на получение доступа к учетной записи главы компании, генерального директора, технического директора и т.д. После получения доступа к таким учетным записям специалисты по фишингу могут продолжать использовать их для связи с другими отделами, например, подтверждать мошеннические банковские переводы любому финансовому учреждению по своему выбору.
- **Фишинг рассылки от Google и Dropbox**. Относительно новое направление фишинговых атак, целью которых являются имена пользователей и пароли для входа в облачные хранилища данных.
- **Фишинговые письма с прикрепленными файлами**. Фишинг-письма с вложениями, содержащими вирусы.
- **Фарминг**. Скрытая переадресация на мошеннический сайт, выполненный с помощью изменения кэша DNS на локальном компьютере или сетевом оборудовании.

Только наличие своевременной и наиболее полной информации о методах хакеров, а также здоровая подозрительность по отношению к необычным, неожиданным сообщениям и предложениям, позволят существенно снизить ущерб от этого вида интернет-мошенничества.

Потому обязательно ознакомьтесь с правилами защиты от фишинга. И прежде всего никому не передавайте свои пароли, заведите привычку всегда вбивать адреса нужных сайтов вручную или пользоваться закладками в браузере, будьте особенно внимательны к ссылкам в письмах.